

No. 5:16-CR-84-1H
No. 5:19-CV-403-H

ORDER

Case 5:16-cr-00084-H Document 121 Filed 09/03/20 Page 1 of 24

at the time of the alleged offense; (2) he did not have the required administrative access to run the damaging malicious code and delete the log files; (3) the chain of custody of the evidence was tainted; and (4) various claims of ineffective assistance of counsel.¹ [DE #106].

COURT'S DISCUSSION

I. Actual Innocence Claims

A. Standard of Review

The government correctly contends petitioner procedurally defaulted on the first three claims by failing to raise them on direct appeal. [DE #117 at 9]. Procedurally defaulted claims can nevertheless be reviewed on federal habeas review if the petitioner first demonstrates "cause" and "actual 'prejudice,'" or that he is "actually innocent." Bousley v. United States, 523 U.S. 614, 622 (1998) (citations omitted). In response to the government's motion to dismiss, petitioner does not raise issues of cause and prejudice, but rather, argues he is actually innocent. [DE #106-1 at 1; DE #120 at 3, 8, 12-13].

"A valid actual innocence claim 'requires petitioner to support his allegations of constitutional error with new reliable evidence - whether it be exculpatory scientific evidence,

¹ Following his conviction by a jury, petitioner fired his counsel and hired new counsel who represented him at sentencing. He appears to mistakenly refer to his sentencing counsel as appellate counsel. However, as no appeal was ever filed, petitioner did not have appellate counsel.

trustworthy eyewitness accounts, or critical physical evidence—that was not presented at trial.” Finch v. McKoy, 914 F.3d 292, 298 (4th Cir. 2019) (quoting Schlup, 513 U.S. at 324). A petitioner must also ‘demonstrate that the totality of the evidence would prevent any reasonable juror from finding him guilty beyond a reasonable doubt, such that his incarceration is a miscarriage of justice.’” Id. (quoting Teleguz v. Pearson, 689 F.3d 322, 329 (4th Cir. 2012) (internal citations omitted)). “[A]ctual innocence’ means factual innocence, not mere legal sufficiency.” Bousley, 523 U.S. at 623-24 (citing Sawyer v. Whitley, 505 U.S. 333, 339 (1992)).

B. Analysis

i. Alibi Evidence

Petitioner relies on the new evidence, not presented at trial of credit card records and the affidavits of two friends who accompanied his family on vacation in Florida. [DE #106-1 at 14-16, 21-22]. This evidence supports his argument that he was actually in Panama City, Florida, between November 22 and 25, 2014, which he contends shows that he was absent from the scene of the crime and therefore innocent.

He contends the alleged scene of the crime was his home in Johns Creek, Georgia. The evidence presented at trial was that petitioner’s computer was used to insert malicious code into Regional Level Application Software System, (“RLAS”) of the United

States Army Reserve Command ("USARC") at 9:57 p.m. and 10:33 p.m. on November 21, 2014 and at 9:04 p.m. on November 23, 2014. The Virtual Private Network ("VPN") logs were presented at trial showing the times a particular computer was connected to the USARC VPN circuit. VPN logs presented at trial provided petitioner's computer was connected to the USARC VPN circuit from 7:54 p.m. on November 21, 2014 to 10:41 a.m. on November 22, 2014. The VPN logs presented at trial also provided petitioner's computer was connected to the USARC network from 8:44 p.m. on November 23, 2014 to 4:53 p.m. on November 24, 2014. Testimony at trial provided a personal identifier, known as a Common Access Card ("CAC"), was required to log in to the RLAS. An Internet Protocol ("IP") address is used to connect a computer to a network. Evidence was presented at trial identifying petitioner's IP address at his home in Georgia. Records known as "centaur logs" were presented at trial of petitioner's specific home IP address showing the times petitioner's home IP address was connected to the USARC VPN circuits. The centaur logs provided petitioner's home IP address was connected to the USARC VPN circuits between approximately 9:47 p.m. and 10:47 p.m. on November 21, 2014.² The centaur logs were filtered for petitioner's home IP address and did not have any entries for November 23, 2014.

² While not presented during direct examination at trial, the centaur logs also show petitioner's home IP address was connected to USARC VPN circuits from 7:53 p.m. on November 21, 2014 to 10:42 a.m. on November 22, 2014.

Petitioner's actual innocence argument of an alibi fails to meet the standard of showing "factual innocence." Petitioner contends that he was in Florida at the time of the November 23, 2014 malicious code modification, and therefore he is innocent. However, he also contends he used his CAC card to login periodically while on vacation, and that he could not be in two places at once. The centaur logs, which show his home IP address was connected to the USARC VPN circuits on November 21, 2014, do not have any entries from his home IP address on November 23 and 24, the dates that he argues he was in Florida. Additionally, the centaur logs only show connection activity between his home IP address and the USARC VPN circuits until 10:42 a.m., on November 22, 2014, the day that he alleges he left for Florida. Therefore, his presence in Florida only corroborates the evidence already admitted at trial.

As to the November 21, 2014 insertion of malicious code, petitioner contends that he does not have evidence, but if the court will grant additional time, he will obtain building logs to show that he was in his office until 9:30 p.m. on November 21, 2014. He contends he lives more than one hour away from his office, and that he would not have been able to drive home in time to allegedly insert the malicious code. However, this argument is not reasonable. The VPN logs, which petitioner contends were fictitiously created, show that his computer was connected to the

USARC VPN circuits from 7:54 p.m. on November 21, 2014 to 10:41 a.m. on November 22, 2014. Additionally, the centaur logs show that it was petitioner's home IP address that accessed the USARC VPN circuits from 7:53 p.m. on November 21, 2014 to 10:42 p.m. on November 22, 2014. While petitioner argues he was in his car driving home from 9:30 to 10:30, the centaur logs show that his home IP address was connected to the USARC VPN circuits. Therefore, this argument, even if supported by building logs evidence, would not "prevent any reasonable juror from finding him guilty beyond a reasonable doubt, such that his incarceration is a miscarriage of justice." Finch, 914 F.3d at 298 (quoting Teleguz, 689 F.3d at 329 (internal citations omitted)).

Next, as new evidence not presented at trial, petitioner has submitted two affidavits, one from James M. Ferguson, Retired Deputy G-1, United States Army Reserve Command, [DE #106-1 at 17-18], and one from Herman F. Whitley, Retired Deputy Director of the G-1, for the United States Army Reserve Command, [DE #106-1 at 19-20]. Both affidavits addressed petitioner's good character and Mr. Ferguson stated his personal disbelief in petitioner being found guilty. Additionally, the affidavit of Mr. Ferguson provided that he was aware of jealousy in the Army Reserve automation and that "[a]s the senior HR person on duty for the USARC for almost two years at Ft. Bragg, I can say without question my experiences with the USARC automation world convinces me Mittesh was set up

because of professional jealousies." [DE #106-1 at 17]. This affidavit supports petitioner's argument that Loren Taylor ("Taylor") had "a compelling and competing interest with an animus relationship against [petitioner]." [DE #120 at 1-2]. Petitioner also contends Taylor had the motive, as Taylor's company lost the RLAS contract bid to Akira. Petitioner argues that Taylor had the requisite access to be able to remotely access petitioner's computer while he was unaware, alter the malicious code, and thereby to frame petitioner. Counsel for petitioner argued at trial and elicited testimony from two witnesses about their observations of unwanted access. Petitioner contends the VPN logs were not logs at all but rather fictitious records that were created by Taylor to frame petitioner. However, as noted above, the centaur logs corroborate the VPN logs. While this testimony regarding professional jealousies may have been useful to petitioner, even if true, does not meet the heavy burden that this information would have "prevent[ed] any reasonable juror from finding him guilty beyond a reasonable doubt, such that his incarceration is a miscarriage of justice." Finch, 914 F.3d at 298 (quoting Teleguz, 689 F.3d at 329 (internal citations omitted)).

ii. Lack of Access Evidence

Finally, petitioner also submitted an affidavit from Kathleen Crocker stating "[i]n order to have done the things that Mr. Das

has been accused of he would have had to have very high access, that he never had to my knowledge." [DE #106-1 at 23]. Ms. Crocker stated "[m]y testimony, if I [were] called or asked, would have been that in order to get Admin Access (Admin CAC) you must have Security Plus Certification along with several other requirements." [DE #106-1 at 23]. She additionally declared "[a]lso, you must have Admin access to remotely login to any server and to delete physical files on the servers." [DE #106-1 at 23]. Petitioner's affiant Kathleen Crocker has not identified herself except as to her residence for two years in Wisconsin and that she "had obtained the [Security Plus] certification, but Laura Reed (COR) denied my request for approval, which shows that it is not easy to gain Admin access." [DE #106-1 at 23]. She further declared "I have met every requirement, then had to meet more requirements, and after trying for nearly six years I got access, but I still have very limited access." [DE #106-1 at 23].

Petitioner also attached an affidavit from Randall Osborn that "[m]y testimony, if I [were] asked, would have been that [to] obtain Admin/DBA Access to USARC servers, you must have a current Security+ Certificate. Admin/DBA access is required to make system or application changes on the servers." [DE #106-1 at 24]. Petitioner contends these affidavits support his argument that he never obtained this Security+ certification and did not have the access to commit the offense.

However, this requirement for obtaining access is not "new" evidence, as defense counsel at trial elicited testimony that obtaining underscore access requires Security+ Certification. [DE #78 at 67-68]. Trial counsel for petitioner elicited testimony that petitioner did not have the requisite access to erase trace logs, from Richard Jacobs, who worked with petitioner on the RLAS. [DE #78 at 58, 68]. Defense counsel elicited testimony from the affiant Randall Osborn, a systems analyst with Tiber Creek at the time of offense, that trace logs could only be deleted by someone with an "underscore account," and he did not know if petitioner possessed that account. [DE #78 at 76, 85]. Defense counsel additionally elicited testimony from Randall Osborn that "if Mittesh didn't coming up and stand in front of me eyeball to eyeball and tell me he did this, I would never believe this." [DE #78 at 91]. The government elicited testimony that petitioner had "administrative or overall access" from Darren Brown, who at the time relevant to the offense was working as a database administrator for RLAS. [DE #76 at 11; #77 at 104-05, 120]. The government also elicited testimony from John Bringolf, a database administrator with Science Applications International Corporation ("SAIC"), that the trace logs could be deleted by someone who had administrative access. [DE #76 at 107]. Petitioner has not

presented new evidence³ on this issue to support his actual innocence claim.

iii. Code on Laptop Not "Malicious"

Petitioner contends this "malicious code" found on his computer was commonly accessed code that anyone could obtain from the internet. [DE #120 at 2]. He also states that "this code was not on the SQL Server where it would execute because [petitioner] did not have the necessary security rights to the server." [DE #120 at 2]. However, the evidence at trial provided that petitioner himself emailed a colleague on November 21, 2014, requesting code to delete a job, and parts of this emailed code were found in the malicious code. [DE #77 at 238-41]. Petitioner contends the malicious code labeled "Time Bomb" was not found on his computer. [DE #120 at 2]. Additionally, testimony elicited from Mr. Osborn at trial provided that the malicious code found was "a very rudimentary code." [DE #78 at 85]. Further testimony elicited at trial from Mr. Osborn provided "If an experienced programmer wanted to crash RLAS, they would have done it in such a way that we would still be looking for it." Id. Indeed, his colleague Darren Brown, who emailed the code to petitioner on November 21, 2014 after petitioner requested it by phone call,

³ The court notes petitioner offers what he thinks an expert's testimony would have been, if he were called at trial, namely that petitioner did not have the requisite access and that the code on his computer was not malicious. However, petitioner has not presented an affidavit from an expert but merely contends this is what an expert would have argued.

testified on direct examination that he sent it "almost immediately because it was just a matter of googling it and dropping it in." [DE #77 at 111]. Petitioner also argues the testimony of Osborn at trial was that he had observed components of the same code twenty years prior and that "the only common factor back th[e]n and this time around is Mr. Loren Taylor with very high level access (God Access)." [DE #120 at 2]. Defense counsel upon cross-examination also elicited testimony from Special Agent Reinecke that this similar code was identified from 2000. [DE #77 at 75-76]. Therefore, petitioner has not supported his argument that this is new evidence.

Petitioner has not met his burden to "demonstrate that the totality of the evidence would prevent any reasonable juror from finding him guilty beyond a reasonable doubt, such that his incarceration is a miscarriage of justice." Finch, 914 F.3d at 298 (quoting Teleguz, 689 F.3d at 329 (internal citations omitted)). As petitioner has not met his burden to show "actual innocence," and has not even made argument as to "cause" or "prejudice," petitioner's first three claims are procedurally defaulted. Bousley, 523 U.S. at 622.

II. Ineffective Assistance of Counsel

Petitioner's fourth claim, ineffective assistance of counsel, includes six subsidiary claims as to trial counsel and one subsidiary claim as to sentencing counsel.⁴

A. Standard of Review

To prove ineffective assistance of counsel, petitioner must satisfy the dual requirements of Strickland v. Washington, 466 U.S. 668, 687 (1984). First, petitioner must show that counsel's performance was deficient in that it fell below the standard of reasonably effective assistance. Id. at 687-88. In making this determination, there is a strong presumption that counsel's conduct was "within the wide range of reasonable professional assistance; that is, the defendant must overcome the presumption that, under the circumstances, the challenged action 'might be considered sound trial strategy.'" Id. at 689 (quoting Michel v. Louisiana, 350 U.S. 91, 101 (1955)). The Strickland court reasoned that, "[i]t is all too tempting for a defendant to second-guess counsel's assistance after conviction or adverse sentence, and it is all too easy for a court, examining counsel's defense after it has proved unsuccessful, to conclude that a particular act or omission of counsel was unreasonable." Id. (citing Engle v. Isaac, 456 U.S. 107, 133-34 (1982)). Second, petitioner "must show that

⁴ As noted previously, petitioner incorrectly refers to sentencing counsel as appellate counsel in his filings.

there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome." Id. at 694.

B. Analysis

i. Alleged Ineffective Assistance of Trial Counsel

As to his first six claims of ineffective assistance of trial counsel, petitioner has failed to show prejudice. These claims of ineffective assistance include trial counsel's failure (i) to call petitioner to testify on his own behalf as well as denying petitioner the constitutional right to testify, [DE #106-1 at 2, 9; DE #120 at 3-7]; (ii) to conduct any pre-trial investigations, which petitioner contends would prove that he was not at the scene of the crime, [DE #106-1 at 4, 7; DE #120 at 8-10]; (iii) to file notice of alibi, [DE #106-1 at 5]; (iv) to call alibi witnesses, [DE #106-1 at 11, 21-22; DE #120 at 7-8, 12-13]; (v) to engage an expert witness after he was paid by petitioner to do so, [DE #106-1 at 3, 4, 10; DE #120 at 10-12]; and (vi) to object to the admissibility of tainted evidence, [DE #106-1 at 8].

a. Defendant's Right to Testify

Petitioner claims that counsel did not advise him of his right to testify at trial; failed to explain to petitioner the "tactical implications of testifying or not testifying;" "perfidiously coerc[ed]" him not to testify and told him that he would not be

testifying; and failed to call him to testify on his own behalf, even though petitioner repeatedly requested to do so. [DE #106-1 at 2, 9; DE #120 at 5].

Petitioner has offered sixteen points that he would have offered were he called to testify: (1) a CAC is unique to each user and can only be used as one login at a time; (2) he was not home in Georgia on November 21, 2014 or on November 22, 23, and 24 when the VPN log stated that he was; (3) he did not have the requisite access to execute the malicious code and delete the security logs; (4) whoever deleted the security log had to have administrative access; (5) retrieval of the CAC log would have shown that he was not logged in when the VPN log showed that he was; (6) he had a contract to oversee the smooth transition of RLAS to the new company; (7) he was going to be paid \$150,000 for the smooth transition; (8) he therefore had no motive to insert malicious code; (9) Loren Taylor lost the bid for RLAS to the new company; (10) some of the malicious code had been introduced nearly twenty years prior, before petitioner worked on RLAS, but when Mr. Taylor, who possess high level access was around; (11) Taylor had the high security level access required to access servers and implant the malicious code, as well as to remotely access petitioner's computer; (12) Taylor retrieved the VPN logs in violation of industry standards and these logs could have been modified once retrieved; (13) witnesses were ready to testify that

petitioner was in Florida, not Georgia, when the malicious code was introduced; (14) trial counsel failed to call alibi witnesses to the stand as instructed; (15) petitioner did not have the requisite access to place the code on the server and trial counsel could have easily obtained the documentation from the AUSA and USAR regarding petitioner's access; and (16) malicious code was not found on petitioner's computer as the code on his computer was common code used for deleting jobs and not "malicious", and that petitioner requested it from Darren Brown as he was going on vacation and "wanted a way to make sure the code only executed once and did not clear out more than it was supposed to do," and that he did not actually use the code provided by Darren Brown in the email. [DE #106-1 at 9; DE #120 at 5-7].

"Because the burden of ensuring that a criminal defendant is informed of the nature and existence of the right to testify rests upon trial counsel, the burden shouldered by trial counsel is a component of effective assistance of counsel." Sexton v. French, 163 F.3d 874, 882 (4th Cir. 1998) (citing Brown v. Artuz, 124 F.3d 73, 79 (2d Cir. 1997)). Even if the allegation were correct that counsel failed to inform petitioner of the existence and nature of his right to testify, petitioner has not shown prejudice under Strickland. Petitioner was advised by the court of his right to testify at the Rule 11 hearing and stated on the record that he understood his rights. [DE #36 at 4, 12]. Petitioner cannot show

prejudice because his first, fourth, the allegation in his third point regarding access to delete the security log, the allegation in his tenth point that the malicious code had existed years ago, the allegation in his eleventh point that Taylor had high level security access, and his sixteenth point regarding using the code for going on vacation, were elicited from the testimony of witnesses at trial [DE #76 at 46-49, 75-76, 107; DE #77 at 69-70, 110, 222; DE #78 at 6, 66, 83-84] and his second, fifth, and twelfth points were contradicted by the centaur logs at trial discussed supra.

Petitioner has not shown prejudice as to his third point regarding his alleged lack of access "to execute the malicious code," considering the weight of the evidence presented at trial. Evidence at trial contradicted such a proffer of testimony as components of malicious code were found on petitioner's computer as a "lost file," that had been deleted from his computer. [DE #77 at 218-23 Govt. Ex. 48]. Additionally, testimony at trial provided there are two types of registries on computers: computer specific and user specific. [DE #77 at 224]. Testimony at trial also provided there are MRU lists, which are lists that detail the most recently accessed files for a program or an individual user. [DE #77 at 224-25]. The MRU list for one of the servers affected by the malicious code included a malicious code file with a location pointing to the USAR framework. [DE #77 at 228-29].

Testimony at trial further provided that petitioner's user account was accessing the USAR Framework at 10:29 p.m. on November 21, 2014. [DE #77 at 232-36]. The malicious code was last modified at 10:33 p.m. on November 21, 2014. [DE #77 at 236]. While petitioner contends that he would have testified that he did not have access to execute the malicious code, he has not alleged prejudice in light of the overwhelming evidence against petitioner at trial.

Petitioner has not alleged prejudice as to points six through sixteen. His allegation in points six through eight that he was to be paid \$150,000 for the smooth transition of the RLAS system and thus lacked motivation to insert malicious code is conclusory and he has alleged no facts to support such an allegation. As to points nine through twelve implicating Taylor in tainting the VPN logs and possessing the high level access to enable him to both access petitioner's computer remotely as well as to implant the malicious code, the court notes counsel already elicited testimony at trial that remote access was possible and that Taylor possessed the high-level access. As to points thirteen and fourteen, the centaur logs did not have entries from petitioner's home IP address, after 10:42 a.m. on November 22, 2014. As to points fifteen and sixteen regarding not having access to place the code on the server and the code on his laptop not being malicious, the court notes these arguments were discussed supra.

Petitioner has not alleged a reasonable probability that the outcome would have been different had he exercised his right to testify, and the record shows significant evidence supporting the jury's finding of guilt.

b. Alleged Failure to Conduct Pre-Trial Investigation and Failure to Call Expert

As to his second and fifth claims of ineffective assistance, petitioner contends his counsel should have obtained the security access documents from the government and should have called an expert to testify. Petitioner contends "[t]he findings from the security access documents will confirm that the movant does not have the operational capability to execute the malicious code and delete the access logs." [DE #106-1 at 7]. As stated above, the government elicited testimony from a witness at trial that petitioner had administrative access. Counsel for petitioner provided evidence at trial from a witness to contradict the government, specifically that petitioner did not have access to delete the trace logs.

As to the fifth claim of ineffective assistance, petitioner contends that his attorney failed to utilize the expert, with whom counsel told petitioner he had reached an agreement on a retainer fee and for whose testimony petitioner paid counsel twenty thousand dollars. [DE #106-1 at 3, 10]. Petitioner contends his trial counsel told him he was unable to have the expert testify at trial

because the expert was indisposed, and yet petitioner was not refunded. [DE #106-1 at 10].

Petitioner contends the expert would have made it plain to the jury that (1) "it was logically impossible for [petitioner] to execute the code and delete the security logs because it required the very high system security level, commonly referred to as 'God Access;' that the [petitioner] did not possess," [DE #106-1 at 10]; (2) the "SQL Batch Deletion Code" is not malicious and "is routinely used throughout the industry to keep a SQL job from executing more than once," [DE #120 at 11]; and (3) "how the Common Access Card (CAC) security log works and how it is the primary log that any forensic auditor would have used while maintaining Chain of Custody." [DE #106-1 at 3].

As to the third proffered point of expert testimony, petitioner has not shown prejudice regarding the expert's testimony about CAC logs. Petitioner contends that the CAC log would show that he was in the office on November 21, 2014, when the fictitious log shows that he was working from home. [DE #106-1 at 4].

As discussed supra, petitioner does not contest the centaur logs that show his home IP address was used during the same time windows as the VPN logs. Petitioner also does not contest the evidence presented at trial in which the code found on his computer was linked to his CAC identification. [DE #77 at 218-23 Govt. Ex.

48]. The evidence at trial presented that petitioner's user account accessed the USAR framework just four minutes prior to the modification of malicious code at petitioner's home IP address. The government presented testimonial evidence that petitioner had administrative access and petitioner himself has admitted that at least administrative access was required to delete the trace logs. [DE #106-1 at 9].

The court notes defendant has not "overcome the presumption that, under the circumstances, the challenged action 'might be considered sound trial strategy.'" Strickland, 466 U.S. at 689.

c. Failure to Provide Alibi Notice

As to his third claim of ineffective assistance, petitioner contends counsel failed to provide an alibi notice. As counsel had no obligation to file such a notice without request from the government, Fed. R. Crim. P. 12.1, this argument is without merit.

d. Failure to Call Alibi Witnesses

As to his fourth claim of ineffective assistance, petitioner contends counsel failed to call alibi witnesses. Petitioner has alleged that on a night during trial that he and counsel were to meet to discuss issues during trial, counsel fell asleep and did not contact petitioner despite repeated petitioner's phone calls during that evening. [DE #106-1 at 5]. However, as discussed supra, petitioner has admitted he logged on and off while on

vacation. Petitioner has not sufficiently alleged facts to show prejudice.

e. Failure to object to VPN logs

As to petitioner's sixth claim of ineffective assistance, petitioner contends that standard procedure for obtaining the VPN logs was not followed. He specifically contends:

In the investigation of this matter, the Virtual Private Network (VPN) log file was retrieved by a third[-]party contractor at the request of another contractor. After receiving the log file from second contractor, the first contractor then converted the files to an Excel spreadsheet and handed it over to the forensics investigator as an authoritative source of information. This Excel spreadsheet is essentially a tainted document which was fraudulently generated against standard industry procedure to preserving chain of custody of evidence. Such tampering of evidence constructively renders this Excel spreadsheet inadmissible in court. It was based on this tainted evidence that the charges against the movant was premised.

[DE #106-1 at 8]. Petitioner further alleges trial counsel's failure to object to admissibility was ineffective assistance. Petitioner again has not shown prejudice as the centaur logs presented at trial corroborated the VPN logs.

ii. Alleged Ineffective Assistance of "Appellate" Counsel

As to his final claim, petitioner contends that trial counsel rendered ineffective assistance by allegedly failing to file a notice of appeal when requested to do so and that "appellate"⁵

⁵ As previously noted, petitioner incorrectly refers to his sentencing counsel as appellate counsel.

counsel rendered ineffective assistance of counsel by failing to file an appeal. [DE #106 at 8; #106-1 at 6]. Counsel has a duty to file an appeal when requested to do so by a client. United States v. Peak, 992 F.2d 39, 41 (4th Cir. 1993) ("[A] criminal defense attorney's failure to file a notice of appeal when requested by his client deprives the defendant of his Sixth Amendment right to the assistance of counsel, notwithstanding that the lost appeal may not have had a reasonable probability of success."). A properly pled allegation of failure to file an appeal after a request to do so typically results in an evidentiary hearing. However, in the instant matter, after the jury verdict, petitioner allegedly asked his counsel about filing an appeal. However, seven days after the jury verdict, petitioner fired this counsel and retained new counsel for sentencing, [DE #68]. Therefore, this appeal discussion occurred more than one year before it was appropriate to file an appeal and with counsel that petitioner fired in the interim. Therefore, counsel who was terminated had no authority to notice an appeal for petitioner.

Petitioner also contends that his sentencing counsel "failed to file any appeal in the Fourth Circuit" and that counsel "did not tell movant that movant's arguments lacked merit and did not file an Anders brief excluding themselves. Trial and [sentencing] counsel abdicated their responsibility to the movant by failing to file an appeal." [DE #106 at 8; #106-1 at 6]. However, petitioner

does not allege in any of his filings that he ever requested that his sentencing counsel file an appeal. Despite the government's argument that petitioner's claim regarding failure to file an appeal lack merit, petitioner did not respond to these arguments in his detailed response. The court finds petitioner has failed to state a claim that he requested that his sentencing counsel file a notice of appeal.

As petitioner has failed to meet his burden to allege that counsel's performance fell below the standard of reasonable assistance and also has failed to show prejudice, his claims for ineffective assistance of counsel should be dismissed.


CONCLUSION

For the foregoing reasons, the government's motion to dismiss, [DE #117], is hereby GRANTED, and petitioner's motion to vacate, [DE #106], is hereby DISMISSED. The clerk is directed to close this case.

A certificate of appealability shall not issue absent "a substantial showing of the denial of a constitutional right." 28 U.S.C. § 2253(c)(2). A petitioner satisfies this standard by demonstrating that reasonable jurists would find that an assessment of the constitutional claims is debatable and that any dispositive procedural ruling dismissing such claims is likewise debatable. Miller-El v. Cockrell, 537 U.S. 322, 336-38 (2003); Slack v. McDaniel, 529 U.S. 473, 484 (2000); Rose v. Lee, 252 F.3d

676, 683-84 (4th Cir. 2001). A reasonable jurist would not find this court's dismissal of Petitioner's § 2255 Motion debatable. Therefore, a Certificate of Appealability is DENIED.

This 2 day of September 2020.

A handwritten signature in black ink, appearing to read "Malcolm J. Howard", is written over a horizontal line.

Malcolm J. Howard
Senior United States District Judge

At Greenville, NC
#35